COPY PREVENTING DEVICE

Publication number: JP11213554

Publication date: 1999-08-06

Inventor: KATO TAKEHISA; KATO HIROSHI; ENDO NAOKI; YAMADA HISASHI; ENDO KENJIRO

Applicant: TOKYO SHIBAURA ELECTRIC CO

Classification:

- international: ***G06F12/14; G09C5/00; G11B20/10; H04L9/32;*** **G06F12/14; G09C5/00; G11B20/10; H04L9/32;** (IPC1-7): G11B20/10; G06F12/14; G09C5/00; H04L9/32

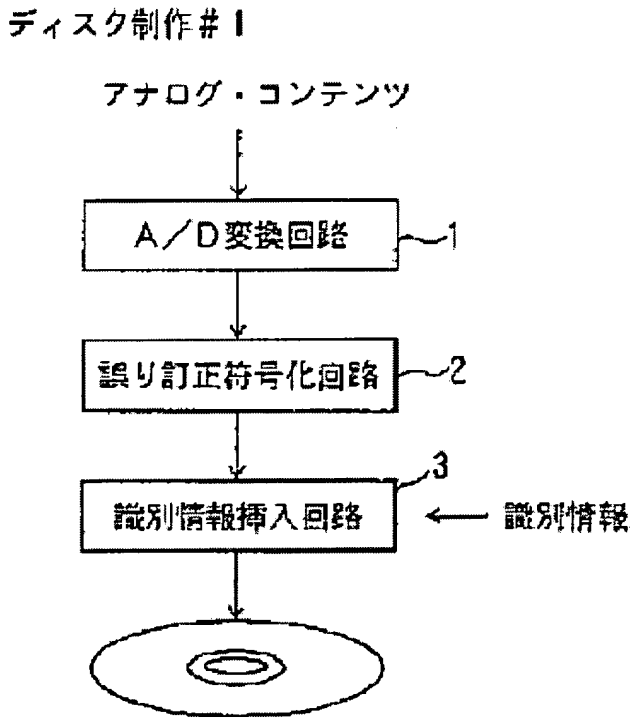
- european:

Application number: JP19980291968 19981014

Priority number(s): JP19980291968 19981014; JP19970361981 19971120

Abstract of **JP11213554**

PROBLEM TO BE SOLVED: To prevent unauthorized copy by recording an identification signal expressing whether contents recorded on an information record medium are original or not in an error-correcting code. SOLUTION: Multimedia data (analog contents) are digitized through precedures of a sampling and quantization, Thereafter, the digital data are subjected to an error-correcting coding in an error-correcting coding circuit 2 in order to correct an error to be generated in a transmission path. Then, an identification signal expressing whether a disk (information recording medium) is original or not is inserted into the digital data data subjected to the error-correcting coding in an identification information inserting circuit 3. In this insertion, specific symbols of analog contents and the idenfication information are replaced and the analog contents into which the identification information are inserted are recorded on the information recording medium.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－213554

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｚ

審査請求　未請求　請求項の数13　ＯＬ　（全 23 頁）

(21)出願番号　特願平10－291968

(22)出願日　平成10年(1998)10月14日

(31)優先権主張番号　特願平9－361981

(32)優先日　平９(1997)11月20日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　加藤　岳久
東京都府中市東芝町１番地　株式会社東芝府中工場内

(72)発明者　加藤　拓
東京都府中市東芝町１番地　株式会社東芝府中工場内

(72)発明者　遠藤　直樹
東京都府中市東芝町１番地　株式会社東芝府中工場内

(74)代理人　弁理士　鈴江　武彦　（外６名）

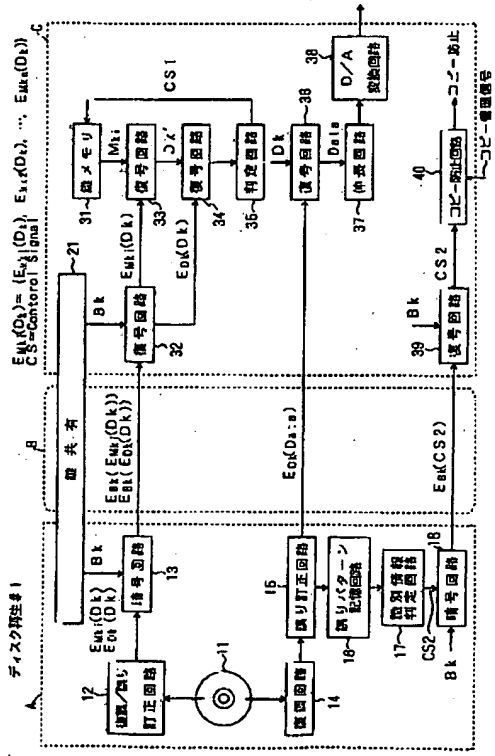
最終頁に続く

(54)【発明の名称】　コピー防止装置

(57)【要約】

【課題】　識別情報を誤り訂正符号に記録しておき、この識別情報をもとに不正なコピーを防止する。

【解決手段】　本発明は、暗号化されたデジタルデータを得る暗号化デジタルデータ獲得部（１５）と、暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出部（１５）と、検出された誤り位置及び誤りシンボル値に基づいて、オリジナルか否かを示す識別情報を検出する識別情報検出部（１６）と、検出された識別情報に基づいて、コピーを防止するか否かを決定する決定部（１７）と、決定結果に基づいて、情報記録媒体のコピーを防止するコピー防止部（４０）とを具備するコピー防止装置である。



【特許請求の範囲】
【請求項１】　暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復調する第１の復調手段と、
前記第１の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る暗号化デジタルデータ獲得手段と、
前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、
前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、前記暗号化及び誤り訂正符号化されたデジタルデータに前記暗号化及び誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、
前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、
前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。
【請求項２】　前記情報記録媒体から前記鍵情報を復号する第１の復号手段と、
前記第１の復号手段により復号された鍵情報に基づいて、前記暗号化デジタルデータ獲得手段によって獲得された暗号化されたデジタルデータからデジタルデータを復号する第２の復号手段と、
前記第２の復号手段により復号されたデジタルデータを再生する再生手段とをさらに具備することを特徴とする請求項１記載のコピー防止装置。
【請求項３】　前記決定手段は、決定結果を示す制御信号を暗号化して出力し、前記コピー防止手段は、前記制御信号を復号し、この復号された制御信号に基づいてコピーを防止することを特徴とする請求項１記載のコピー防止装置。
【請求項４】　前記識別情報は、誤り訂正符号化された後のデジタルデータのうち、所定のシンボルと置き換えられることを特徴とする請求項１記載のコピー防止装置。
【請求項５】　前記決定手段は、
前記識別情報検出手段により検出された識別情報をカウントするカウント手段と、
前記カウント手段によりカウントされた識別情報の数が所定の値を超えているか否かを判定する判定手段と、
前記判定手段による判定結果に基づいて、コピーを防止するか否かを決定する決定手段とを具備することを特徴とする請求項１記載のコピー防止装置。
【請求項６】　前記決定手段は、前記識別情報検出手段により検出された識別情報の位置情報に基づいて、コピーを防止するか否かを決定することを特徴とする請求項１記載のコピー防止装置。
【請求項７】　前記決定手段は、
決定結果を示す制御信号を乱数を使用して所定の演算を行うことにより第１の制御信号に変換する第１の変換手段と、
前記第１の変換手段により変換された第１の制御信号を暗号化する第１の暗号化手段と、
前記乱数を暗号化する第２の暗号化手段とを具備し、
前記コピー防止手段は、
前記第１の暗号化手段により暗号化された第１の制御信号を復号する第１の復号手段と、
前記第２の暗号化手段により暗号化された乱数を復号する第２の復号手段と、
前記第１の復号手段により復号された第１の制御信号を、前記第２の復号手段により復号された乱数を使用して前記所定の演算を行うことにより、前記制御信号に変換する第２の変換手段と、
前記第２の変換手段により変換された制御信号に基づいてコピーを防止する手段とを具備することを特徴とする請求項１記載のコピー防止装置。
【請求項８】　前記識別情報は誤り訂正符号であり、前記識別情報検出手段は、検出された識別情報を誤り訂正符号の誤り訂正能力を利用して訂正することを特徴とする請求項１記載のコピー防止装置。
【請求項９】　暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第１の復調手段と、
前記第１の復調手段により復調された前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに外符号の誤り訂正処理を行なうことにより暗号化及び内符号により誤り訂正符号化されたデジタルデータを獲得する第１の獲得手段と、
前記第１の獲得手段による誤り訂正処理において得られる前記暗号化及び内符号により誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、
前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、前記暗号化及び内符号により誤り訂正符号化されたデジタルデータに前記暗号化及び内符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、
前記識別情報検出手段により検出された識別情報に基づ

いて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。

【請求項１０】　暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第１の復調手段と、

前記第１の復調手段により復調された前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに外符号の誤り訂正処理を行なうことにより暗号化及び内符号により誤り訂正符号化されたデジタルデータを獲得する第１の獲得手段と、

前記第１の獲得手段による誤り訂正処理により得られる暗号化及び内符号により誤り訂正符号化されたデジタルデータにおける第１の誤り位置及び第１の誤りシンボル値を検出する第１の検出手段と、

前記第１の獲得手段により得られた前記暗号化及び内符号により誤り訂正符号化されたデジタルデータに内符号による誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る第２の獲得手段と、

前記第２の獲得手段による誤り訂正処理により得られる暗号化されたデジタルデータにおける第２の誤り位置及び第２の誤りシンボル値を検出する第２の検出手段と、

前記第１の検出手段により検出された第１の誤り位置及び第１の誤りシンボル値、前記第２の検出手段により検出された第２の誤り位置及び第２の誤りシンボル値に基づいて、前記暗号化及び誤り訂正符号化されたデジタルデータに前記暗号化及び積符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、

前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、

前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。

【請求項１１】　暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第１の復調手段と、

前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに前記暗号化及び積符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報のパターンに基づいて、前記第１の復調手段により復調された前記暗号化及び積符号により誤り訂正符号化されたデジタルデータにおける識別情報を検出する識別情報検出手段と、

前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、

前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。

【請求項１２】　暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復調する第１の復調手段と、

前記第１の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る暗号化デジタルデータ獲得手段と、

前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、

前記暗号化デジタルデータ獲得手段により得られた暗号化されたデジタルデータを復号することによりデジタルデータを得る復号手段と、

前記復号手段により得られたデジタルデータに透かし情報として埋め込まれた識別情報の位置情報を抽出する抽出手段と、

前記検出手段により検出された誤り位置及び誤りシンボル値、前記抽出手段により抽出された識別情報の位置情報に基づいて、前記暗号化及び誤り訂正符号化されたデジタルデータに前記暗号化及び誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、

前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、

前記決定手段による決定結果に基づいて、コピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。

【請求項１３】　暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復調する第１の復調手段と、

前記第１の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る暗号化デジタルデータ獲得手段と、

前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、

前記情報記録媒体に格納された暗号化された鍵情報を圧縮する圧縮手段と、
前記圧縮手段により圧縮された鍵情報、前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、識別情報を抽出する抽出手段と、
前記抽出手段により抽出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、
前記決定手段による決定結果に基づいて、コピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、記録媒体上に記録されたマルチメディア・データが、オリジナルなものであるのか、コピーされたものであるのかを判定し、コピーされたものである媒体からの再生であると判定された場合には、コピーを禁止するなどして、不正なコピーを防止するコピー防止装置に関する。

【0002】

【従来の技術】従来、DAT(Digital Audio Tape) やMD(Mini Disc) のようなディジタル記録媒体においては、オリジナルなものからであれば一度限りのディジタル・コピーが可能である。しかし、コピーされたものからの再度のコピー（孫コピー）を作成することはできないようになっている。

【0003】このシステムを、CGMS(Copy Generation Management System) やSCMS(SingleCopy Management System) と呼ぶ。これらは、コピーされたものか否か（コピー可能か否か）を、2ビットのフラグで示すものである。

【0004】

【発明が解決しようとする課題】しかし、このようなCGMSやSCMSは、伝送途中で改竄をうけ、不正コピーされる場合があり、不正にコピーされた、一般に海賊版と呼ばれる媒体が流通する、という問題が有る。

【0005】上述したように、従来の不正コピー防止手段では、伝送途中で改竄をうけ、不正コピーされる場合があり、不正にコピーされた、一般に海賊版と呼ばれる媒体が流通する、という問題がある。

【0006】

【課題を解決するための手段】本発明は、上記実情に鑑みてなされたものであり、情報記録媒体に記録されたコンテンツが、オリジナルなものであるか否かを示す識別情報を誤り訂正符号に記録しておき、この識別情報をもとに不正なコピーを防止するコピー防止装置を提供することを目的とする。

【0007】したがって、まず、本発明の第1の発明によれば、暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、前記第1の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る暗号化デジタルデータ獲得手段と、前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、前記暗号化及び誤り訂正符号化されたデジタルデータに前記暗号化及び誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【0008】また、本発明の第2の発明によれば、暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第1の復調手段と、前記第1の復調手段により復調された前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに外符号の誤り訂正処理を行なうことにより暗号化及び内符号により誤り訂正符号化されたデジタルデータを獲得する第1の獲得手段と、前記第1の獲得手段による誤り訂正処理において得られる前記暗号化及び内符号により誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、前記暗号化及び内符号により誤り訂正符号化されたデジタルデータに前記暗号化及び内符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【0009】さらに、本発明の第3の発明によれば、暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第1の復

調手段と、前記第１の復調手段により復調された前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに外符号の誤り訂正処理を行なうことにより暗号化及び内符号により誤り訂正符号化されたデジタルデータを獲得する第１の獲得手段と、前記第１の獲得手段による誤り訂正処理により得られる暗号化及び内符号により誤り訂正符号化されたデジタルデータにおける第１の誤り位置及び第１の誤りシンボル値を検出する第１の検出手段と、前記第１の獲得手段により得られた前記暗号化及び内符号により誤り訂正符号化されたデジタルデータに内符号による誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る第２の獲得手段と、前記第２の獲得手段による誤り訂正処理により得られる暗号化されたデジタルデータにおける第２の誤り位置及び第２の誤りシンボル値を検出する第２の検出手段と、前記第１の検出手段により検出された第１の誤り位置及び第１の誤りシンボル値、前記第２の検出手段により検出された第２の誤り位置及び第２の誤りシンボル値に基づいて、前記暗号化及び誤り訂正符号化されたデジタルデータに前記暗号化及び積符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【００１０】さらに、本発明の第４の発明によれば、暗号化及び積符号により誤り訂正符号化されたデジタルデータ、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータを復調する第１の復調手段と、前記暗号化及び積符号により誤り訂正符号化されたデジタルデータに前記暗号化及び積符号により誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報のパターンに基づいて、前記第１の復調手段により復調された前記暗号化及び積符号により誤り訂正符号化されたデジタルデータにおける識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、前記情報記録媒体のコピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【００１１】さらに、本発明の第５の発明によれば、暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復調する第１の復調手段と、前記第１の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る暗号化デジタルデータ獲得手段と、前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、前記暗号化デジタルデータ獲得手段により得られた暗号化されたデジタルデータを復号することによりデジタルデータを得る復号手段と、前記復号手段により得られたデジタルデータに透かし情報として埋め込まれた識別情報の位置情報を抽出する抽出手段と、前記検出手段により検出された誤り位置及び誤りシンボル値、前記抽出手段により抽出された識別情報の位置情報に基づいて、前記暗号化及び誤り訂正符号化されたデジタルデータに前記暗号化及び誤り訂正符号化されたデジタルデータの一部と入れ替えて記録され、オリジナルか否かを示す識別情報を検出する識別情報検出手段と、前記識別情報検出手段により検出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、コピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【００１２】さらに、本発明の第６の発明によれば、暗号化及び誤り訂正符号化されたデジタルデータ、前記暗号化及び誤り訂正符号化されたデジタルデータのための暗号化された鍵情報が記録された情報記録媒体から、前記暗号化及び誤り訂正符号化されたデジタルデータを復調する第１の復調手段と、前記第１の復調手段により復調された前記暗号化及び誤り訂正符号化されたデジタルデータに誤り訂正処理を行なうことにより暗号化されたデジタルデータを得る暗号化デジタルデータ獲得手段と、前記暗号化デジタルデータ獲得手段による誤り訂正処理により得られる前記暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置及び誤りシンボル値を検出する検出手段と、前記情報記録媒体に格納された暗号化された鍵情報を圧縮する圧縮手段と、前記圧縮手段により圧縮された鍵情報、前記検出手段により検出された誤り位置及び誤りシンボル値に基づいて、識別情報を抽出する抽出手段と、前記抽出手段により抽出された識別情報に基づいて、コピーを防止するか否かを決定する決定手段と、前記決定手段による決定結果に基づいて、コピーを防止するコピー防止手段とを具備することを特徴とするコピー防止装置、である。

【００１３】

【発明の実施の形態】以下、本発明の実施形態を図面を用いて説明する。

【００１４】本実施形態においては、情報記録媒体は、MDやDVD-RAM などの記録再生可能な媒体を意味する。また、本実施形態においては、元となる画像や音声などの

マルチメディア・データが、アナログ・データであるものとする。

【００１５】＜第１の実施の形態＞図１は、本発明の第１の実施形態におけるコピー防止装置において使用されるディスクの制作の過程を説明するための図である。

【００１６】アナログデータであるマルチメディア・データ（アナログ・コンテンツ）は、A/D 変換回路１にて標本化や量子化の手順を経て、ディジタル化される。その後、伝送路中にて発生する誤りを訂正するために、誤り訂正符号化回路２　にて誤り訂正符号化される。

【００１７】誤り訂正符号化については、「符号理論」宮川、岩垂、今井共著　昭晃堂に詳しい。誤り訂正符号化されたディジタル・データには、ディスク（情報記録媒体）がオリジナルであるか否かを示す識別情報が識別情報挿入回路３にて挿入される。

【００１８】ここでの挿入は、図２に示すように、特定のアナログコンテンツのシンボルと識別情報とが置き換えられるものである。そして、識別情報が挿入されたアナログコンテンツが情報記録媒体に記録される。図２では、データ部のシンボルのｍ番目からｎ番目のシンボルが、それぞれ識別情報DIo,・・・,DIj　に入れ替えられる例を示している。

【００１９】なお、図２に示した例においては、連続するシンボルのパターンが識別情報と置き換えられているが、ある特定のシンボルを識別情報と置き換えても良いし、連続するシンボルではなく何シンボルか空けたシンボル（例えば１シンボル空けて）を識別情報と置き換えてもよい。

【００２０】またデータ部だけでなく、パリティ部のシンボルと入れ替えても構わない。ただし、入れ替えるシンボル数は訂正能力の限界を超えてはならず、訂正能力に余裕を持たせるようにした方が望ましい。

【００２１】次に、誤り訂正符号の特定シンボルが識別情報に入れ替えられたディスクの再生について説明する。

【００２２】図３は、本発明の第１の実施の形態に係る装置を示す図である。

【００２３】なお、DVD(Digital Video Disc, Digital Versatile Disc) には、すでに不正コピー防止のための暗号技術が導入されている。これらの技術については、「DVD 著作保護システム」館林、松崎、石原、福島、映像情報メディア学会技術報告、1997.5.22 , P.15-19 、または「DVD 、パソコン載る」日経エレクトロニクス、1997.8.18(no.696) , p.110-120 、に詳細に述べられている。本実施形態においては、概保護技術の説明を省略する。

【００２４】文献に依れば、DVD では三種の暗号鍵を用いてコンテンツを保護しているが、本実施形態では説明の簡略化のために、２つの暗号鍵を用いて説明する。もちろん、１種のみの暗号鍵、３種以上の複数の暗号鍵、であったとしても、本実施の形態を適用することができる。

【００２５】図３において、AはDVD ディスクドライブ、Bはバスインターフェース、Cは、例えば画像であればMPEG2 復号ユニットのような復号ユニットである。

【００２６】DVD ディスク１１から、暗号化された鍵情報であるEMki(Dk)とEDk(Dk) が読み出される。そして、復調／誤り訂正回路１２によって、読み出された暗号化された鍵情報EMki(Dk)とEDk(Dk) の復調、誤り訂正処理が行われる。

【００２７】暗号化された鍵情報EMki(Dk)とEDk(Dk) 以外の暗号化されたコンテンツ情報EDk(Data) は、復調回路１４によって復調される。

【００２８】一時暗号鍵Bkは、鍵共有プロトコル２１にてDVD ディスクドライブＡと復号ユニットＣ間で共有される。

【００２９】一時暗号鍵Bkを共有したら、暗号化された鍵情報EMki(Dk)とEDk(Dk) を一時暗号鍵Bkで暗号化回路１３にて暗号化し、EBk(EMki(Dk)) とEBk(EDk(Dk))とを復号ユニットＣへ送る。

【００３０】さて、復号ユニットＣの復号回路３２では、EBk(EMki(Dk)) とEBk(EDk(Dk))を共有した一時暗号鍵Bkを用いて復号する。そして、鍵メモリ３１に納められたｎ個のマスタ鍵Mki(i=1,・・・,n) を順次呼び出し、EMki(Dk)を復号回路３３にて復号する。

【００３１】復号回路３３による復号の結果得られたDk'を復号鍵として、復号回路３４にてEDk(Dk) を復号する。そして、復号回路３４による復号により得られた結果と復号回路３３による復号の結果得られたDk'とを判定回路３５で比較し、一致すればDkを暗号化したマスタ鍵を特定でき、かつデータを暗号化した暗号鍵Dkを得られる。一致しなければ、制御信号CS1 にて鍵メモリから新たなマスタ鍵を取り出し、上記手順を繰り返す。

【００３２】一方、復調回路１４にて復調された暗号化データEDk(Data) は、誤り訂正回路１５にて誤り訂正処理を受ける。そして、誤り訂正回路１５において誤り訂正処理を施された暗号化されたEDK(Data) は、復号ユニットＣへ伝送される。

【００３３】誤り訂正回路１５では、誤り訂正処理中に得られる暗号化及び誤り訂正符号化されたデジタルデータにおける誤り位置および、誤りシンボル値を取り出し、この取り出された誤り位置及び誤りシンボル値を誤りパターン記憶回路１６に記憶する。

【００３４】そして、誤りパターン記憶回路１６に記憶された誤り検出位置および誤り訂正前のシンボル値とから、情報記録媒体に識別情報が存在するか否かを識別情報判定回路１７にて調べる。この判定方法について、他の実施の形態とともに、後にまとめて説明する。

【００３５】識別情報判定回路１７における判定結果を示す制御信号ＣＳ２は、暗号回路１８にて先に共有され

た一時暗号鍵Bkを暗号鍵としてEBK(CS2)に暗号化され、復号ユニットＣへ伝送される。

【００３６】復号ユニットＣにおける復号回路３９では、受信したEBK(CS2)を一時鍵Bkを復号鍵として復号回路３９にて復号し制御信号CS2 を得る。

【００３７】そして、コピー防止回路４０は、復号回路３９から出力される制御信号ＣＳ２と、例えば、ＣＧＭＳにおけるコピー管理信号とに基づいて、コピー可能か否かを判定し、コピー不可能であればコピーできないようにする。

【００３８】例えば、D/A 変換回路３８の手前で、タッピングなどの技術を用いてデータを取り、記録したディスクであるならば、誤り訂正回路を通っているので、識別情報は存在しない。その結果、コピー防止回路４０によりコピーが防止される。

【００３９】すなわち、D/A 変換回路３８の手前で採取されたデータは、識別情報と入れ替える前のシンボルに変わっている。従って、識別情報は特定位置にはなく、コピーされたディスクであることが判定できる。

【００４０】誤り訂正された暗号化されたデータEDk(Data)は、バスインターフェースＢを通して復号ユニットＣへ送られる。そして、復号ユニットＣでは、判定回路３５により得られたDkを用いて復号回路３６にて暗号化されたデータEDk(Data) を復号する。

【００４１】復号されたDataは、伸長回路３７にて伸長され、さらにD/A 変換回路３８にてアナログデータに変換されて、ディスプレイ（図示せず）やアンプを通じてスピーカ（図示せず）により再生される。

【００４２】＜第２の実施の形態＞上述の実施の形態においては、通常の誤り訂正符号の場合を説明した。しかしながら、マルチメディアなどのディジタルデータでは、現在ほとんどが２重符号化誤り訂正符号を用いて誤り訂正符号化されている。そこで、次に２重符号化誤り訂正の場合の実施形態について説明する。

【００４３】図４に、一般的な積符号の符号化および復号化の流れを示す。

【００４４】積符号の場合、二次元的にシンボルを配列することによって構成される。図４のごとく、まず行方向に誤り訂正符号化されて、内符号ができる。

【００４５】次に、列方向に誤り訂正符号化されて外符号ができる。そして、これを伝送する。受信された積符号は、外符号が復号され、次に内符号が復号される。このとき、外符号の復号の際に誤り訂正不可能と判定された場合は、その列すべてにフラグと呼ばれるビットをたてて、誤りの存在を示す。内符号の復号の際に、そのフラグが立っているシンボルは消失したものとして訂正することで、訂正能力を増すことができる。これが消失訂正である。

【００４６】図５は、積符号を使用した場合の情報記録媒体の製造手順を示す図である。

【００４７】これまでと同様に、アナログ・コンテンツはA/D 変換回路５１にてディジタル情報に変換される。そして、内符号符号化回路５２にて誤り訂正符号化される。そして、識別情報が規則に従って識別情報挿入回路５３にてデジタルデータのうちの所定のシンボルと入れ替えられる。

【００４８】次に、内符号により誤り訂正符号化され、識別情報が挿入されたデジタルデータは、外符号符号化回路５４にて符号化され、その後、変調回路５５により変調処理を受け、情報記録媒体に記録される。ここで、識別情報の挿入の方法については後述する。

【００４９】図６は、本発明の第２の実施の形態に係るコピー防止装置を示す図である。なお、図６において、図３と同一部分には同一符号を付し、その説明を省略する。

【００５０】同図において、一時鍵＆データ暗号鍵判定部６１は、図３に示した復調／誤り訂正回路１２、暗号回路１３、鍵共有２１、復号回路３２、鍵メモリ３１、復号回路３３，３４及び判定回路３５を１つのセクションで表したものである。

【００５１】DVD ディスク１１から、暗号化された鍵情報であるEMki(Dk)とEDk(Dk) が読み出される。そして、図３において説明した場合と同様に、一時鍵生成とデータ暗号鍵の判定が一時鍵＆データ暗号鍵判定部６１にて行われ、一時鍵Bkとデータ暗号鍵Dkが得られる。

【００５２】DVD ディスク１１に記録された暗号化データEDk(Data) は、復調回路１４により復調され、さらに外符号誤り訂正回路６２により外符号の誤り訂正処理を受ける。

【００５３】このとき、外符号誤り訂正処理が済んだデータは、識別情報検出回路６４にて識別情報メモリ６３に記録された識別情報のパターンと比較され、識別情報DIが取り出される。

【００５４】そして、識別情報判定回路６５にてオリジナルディスクかコピーであるかを判定して、制御信号CS2 を出力する。出力された制御信号CS2 は、一時鍵Bkを暗号鍵として暗号回路１８にて暗号化され、この暗号化されたEBk(CS2)は復号ユニットＣに伝送される。

【００５５】伝送されたEBk(CS2)は、一時鍵Bkを復号鍵として復号回路３９により復号され制御信号CS2 が得られる。コピー防止回路４０は、制得信号CS2 とコピー管理信号とから、コピー可能か否かを判定し、コピー不可能であればコピーできないようにする。

【００５６】一方、外符号誤り訂正回路６２により外符号誤り訂正処理を受けた暗号化データは、識別情報を抽出された後、そのシンボルにフラグが立てられる。そして、このフラグは、内符号誤り訂正回路６６における内符号誤り訂正処理にて消失訂正を受ける。

【００５７】こうして誤り訂正された暗号化データは、復号ユニットＣに伝送される。伝送された暗号化データ

は、復号回路３６にて復号され、伸長回路３７にて伸長され、さらにD/A 変換回路３８　にてアナログデータに変換されて、ディスプレイ（図示せず）やスピーカ（図示せず）を通して再生される。

【００５８】例えば、D/A 変換回路の手前で、タッピングなどの技術を用いてデータを取り、記録したディスクであるならば、誤り訂正回路６２，６６を通っているので、識別情報は存在しない。

【００５９】すなわち識別情報と入れ替える前のシンボルに変わっているはずである。従って、識別情報は特定位置にはなく、コピーされたディスクであることが判定できる。

【００６０】＜第３の実施の形態＞上述の第２の実施形態では、外符号復号において識別情報を取り出す方式になっている。このため、誤り訂正符号の信頼度が低い（誤訂正確率や訂正不能確率が高い）という問題がある。

【００６１】また、識別情報をメモリに予め記録されているパターンとの比較により取り出すという方式であるため、誤訂正した場合や訂正不能であった場合に、識別情報を誤検出してしまう確率が高くなるという問題がある。

【００６２】そこで上記問題点を解決する、積符号を利用した場合の第３の実施形態について説明する。

【００６３】積符号を用いた場合の情報記録媒体の制作手順を図７に示す。図５と異なるのは、識別情報挿入回路５３の位置である。

【００６４】アナログ・コンテンツは、A/D 変換回路５１にてディジタル情報に変換される。そして、内符号符号化回路５２にて誤り訂正符号化され、次に外符号符号化回路５４にて符号化される。

【００６５】そして、識別情報が規則に従って識別情報挿入回路５３にて入れ替えられ、変調回路５５で変調処理を受け、情報記録媒体に記録される。ここで、識別情報の挿入の方法について後述する。

【００６６】次に、図７に示した方法により制作されたDVD ディスクを再生するコピー防止装置について説明する。

【００６７】図８は、本発明の第３の実施の形態に係るコピー防止装置を示す図である。なお、図６と同一部分には同一符号を付し、その説明を省略する。

【００６８】DVD ディスク１１から、暗号化された鍵情報であるEMki(Dk)とEDk(Dk）が読み出される。そして、一時鍵生成とデータ暗号鍵の判定が一時鍵＆データ暗号鍵判定部６１にて行われ、一時鍵Bkとデータ暗号鍵Dkが得られる。

【００６９】DVD ディスク１１　に記録された暗号化データEDk(Data) は、復調回路１４により復調され、さらに外符号誤り訂正回路７１により外符号誤り訂正処理を受ける。

【００７０】また、外符号誤り訂正回路７１は、誤り訂正処理時に得られる誤り位置情報と訂正前の誤りシンボル値を誤りパターン記憶回路７３へ送る。

【００７１】次に、外符号誤り訂正処理が行われたデジタルデータに対して内符号誤り訂正回路７２にて内符号誤り訂正処理が行われ、外符号誤り訂正と同様に、内符号誤り訂正回路７２は内符号誤り訂正処理において得られる誤り位置情報と訂正前の誤りシンボル値を誤りパターン記憶回路７３へ送る。

【００７２】こうして誤り訂正の結果得られた誤り位置情報と訂正前の誤りシンボル値と、識別情報メモリ７４からの識別情報とから、識別情報検出回路７５にて識別情報が検出される。

【００７３】そして、識別情報判定回路７６にて識別情報が存在するか否かの判定が行われ、この判定結果を示す制御信号CS2 が出力される。なお、識別情報判定回路７６における判定の方法について後述する。

【００７４】制御信号CS2 は、一時鍵Bkを暗号鍵として暗号回路１８にて暗号化されて復号ユニットＣへ伝送される。暗号化された制御信号EDK(CS2)　は、復号回路３９にて復号され制御信号CS2 が取り出され、コピー防止回路４０に出力される。

【００７５】また、誤り訂正処理された暗号化されたデータEDk(Data) は、復号ユニットＣへ伝送され、伝送されたEDk(Data) は、一時鍵生成＆データ暗号鍵判定部６１にて得られたDkを用いて、復号回路３６にてEDk(Data) を復号する。続いて、伸長回路812 にて圧縮されたデータが伸長され、さらにD/A 変換回路３８にてアナログデータに変換されて、ディスプレイ（図示せず）やスピーカ（図示せず）を通して再生される。

【００７６】例えば、D/A 変換回路３８の手前で、タッピングなどの技術を用いてデータを取り、記録したディスクであるならば、誤り訂正回路を通っているので、識別情報は存在しない。

【００７７】すなわち、識別情報は、識別情報と入れ替える前のシンボルに変わっているはずである。従って、識別情報は特定位置にはなく、コピーされたディスクであることが判定できる。

【００７８】こうして得られた制御信号CS2 をもとに、コピー防止回路４０は、制御信号CS2 とコピー管理信号（図示せず）とから、コピー可能か否かを判定し、コピー不可能であればコピーできないようにする。

【００７９】＜第４の実施の形態＞第３の実施の形態においては、誤り訂正処理を終えた後に識別情報を取り出すコピー防止装置を示した。ここでは、第４の実施形態として、誤り訂正前に識別情報を取り出すコピー防止装置を示す。

【００８０】図９は、本発明の第４の実施の形態に係るコピー防止装置を示す図である。同図において、図８と同一部分には、同一符号を付し、その説明を省略する。

【００８１】DVD ディスク１１から、鍵情報であるEMki(Dk)とEDk(Dk) が読み出される。そして、一時鍵生成とデータ暗号鍵の判定が一時鍵＆データ暗号鍵判定部６１にて行われ、一時鍵Bkとデータ暗号鍵Dkが得られる。

【００８２】DVD ディスク１１に記録された暗号化されたデータEDk(Data) は復調回路１４により復調される。復調された暗号化データは、例えば積符号ブロック単位に識別情報メモリ８１に記録されている識別情報とのパターン比較が識別情報検出回路８２にて行われる。

【００８３】ここで識別情報が検出されれば、識別情報DIを暗号回路８３にて一時鍵Bkで暗号化し復号ユニットＣへ送る。

【００８４】復号ユニットＣにおける復号回路８６では、一時鍵BKを復号鍵として暗号回路８３で暗号化された識別情報DIを復号し、識別情報判定回路８７へ送る。識別情報判定回路８７は、識別情報DIに基づいてオリジナルであるかコピーされたディスクであるかを判定し、この判定結果を示す制御信号CS2 を出力する。この判定方法については後述する。

【００８５】コピー防止回路４０は、制御信号CS2 とコピー管理信号とから、コピー可能か否かを判定し、コピー不可能であればコピーできないようにする。この様に、識別情報を復号ユニットＣへ暗号化して送り、復号ユニット側で判定することにより、識別情報から制御信号がどのようにして出力されるかを、ディスク・ドライブ制作会社から隠蔽することが可能となる。

【００８６】復調された暗号化されたデータEDk(Data) は、外符号誤り訂正回路８４　、内符号誤り訂正回路８５　により、それぞれ誤り訂正処理を受け、復号ユニットＣへ伝送される。

【００８７】伝送されたEDk(Data) は、既に得られたDkを用いて、復号回路３６にて復号される。そして、伸長回路３７にて圧縮されたデータが伸長され、さらにD/A変換回路３８にてアナログデータに変換されて、ディスプレイ（図示せず）やスピーカ（図示せず）を通して再生される。

【００８８】例えば、D/A 変換回路３８の手前で、タッピングなどの技術を用いてデータを取り、記録したディスクであるならば、誤り訂正回路８４，８５を通っているので、識別情報は存在しない。

【００８９】すなわち、識別情報は、識別情報と入れ替える前のシンボルに変わっているはずである。従って、識別情報は特定位置にはなく、コピーされたディスクであることが判定できる。

【００９０】＜積符号の場合の識別情報の挿入方法＞次に、積符号の場合の識別情報の挿入方法について説明する。ここで、識別情報は１シンボルでも複数シンボルでも構わない。複数シンボルである場合は、予め定められた異なるシンボルにしても構わない。

【００９１】まず、最も簡単な積符号の特定位置に識別情報を挿入する場合について説明する。

【００９２】図５においては、ある１シンボルを識別情報シンボルとしている。識別情報シンボルとしては、複数存在しても構わない。これまで説明したように、メモリ内に識別情報シンボルを登録しておき、どの識別情報シンボルかを特定すればよいだけである。

【００９３】図１０の場合、積符号のｉ番目の列のシンボルが全て識別情報であることが予め判明しているため、外符号の復号処理にてｉ番目の復号は行わず、フラグを立てるだけの処理にしても構わない。このような場合、内符号の復号処理ではｉ番目のシンボルは、全て消失シンボルとして扱われることになる。

【００９４】逆にある特定の行が全て識別情報であってもよい。この場合は、外符号で誤り訂正が行われてしまうため、例えば図８に示したコピー防止装置のごとく誤り位置と誤りシンボル情報を記憶しておき、識別情報メモリに登録されている識別情報との一致を調べるか、図９に示したコピー防止装置のごとく誤り訂正前に積符号ブロック単位に識別情報シンボルとのパターン比較を行うこととなる。

【００９５】次に、常に第ｉ番列のシンボルに特定する必要はなく第ｊ行は第ｉ列というようなルールに従って挿入する方法について説明する。

【００９６】図１１に示すように、外符号の誤り訂正能力未満のシンボル数だけ、例えば外符号が５シンボル以上誤り訂正可能である場合に、第ｊ、ｋ、ｌ行の第ｉ列に識別情報を挿入する（ここでは、積符号ブロック内に３シンボル挿入される）ようにしておく。

【００９７】識別情報検出時に、後述する識別情報判定処理を行うことにより、オリジナルかコピーかを判定することが可能となる。

【００９８】また、図６に示したコピー防止装置の場合には、識別情報に誤りが発生した場合にも外符号の復号処理で誤り訂正が可能で、識別情報が得られなくなる場合を減らすことが可能となる。しかし、この場合は外符号の情報部にのみ挿入し、挿入後に外符号符号化を行う必要がある。

【００９９】上記２つの識別情報挿入方法の場合、特定位置に識別情報を埋め込んでいるため、識別情報挿入位置が漏洩した場合、不正コピーが可能となる場合がある。

【０１００】そこで、次に、識別情報の埋め込み位置を変化させる方法を説明する。

【０１０１】例えば、図１２のごとく、ある複数シンボルのパターンを識別情報とする場合に、積符号ブロック単位ごとに、決められた個数のシンボルパターンを挿入する。識別情報を取り出すときに、積符号ブロックの中で得られたシンボルパターンの個数を計算し、その個数がある閾値以上になればオリジナルであると判定するようにしてもよい。

【0102】次に、複数のシンボルパターンによる識別情報の挿入方法について説明する。例えば、図13に示すように、積符号のブロックに複数のシンボルパターンを挿入しておき、検出する際に予め登録された識別情報シンボルパターンと照合するようにする。

【0103】このシンボルパターンは、それぞれが異なるシンボルパターンでも構わないし、同じシンボルがnシンボル（例えば n=5）続くパターンにしても構わない。この場合、識別情報の抽出は、あるシンボルが連続してnシンボル現れたら、それは識別信号であると判定すれば良い。

【0104】この識別信号の検出には、誤り訂正前に検出を行う図9の方法や、内符号誤り訂正前に検出を行う図6の方法も可能であるが、位置が変化するために誤り位置情報が正確な図8の方法、すなわち誤り位置情報と誤りシンボル情報とから識別信号を検出する方法が好ましい。

【0105】また、前記積符号に識別情報としてのシンボルを挿入する位置は、それぞれが重ならないように異なる位置に挿入する必要がある。

【0106】＜識別情報の判定方法＞次に、識別情報の判定方法について説明する。

【0107】図14は、識別情報の判定方法を説明するためのフローチャートである。

【0108】図14に示すように、例えば積符号ブロック単位で登録された識別情報がいくつ検出されたかを計算し（ｓｔｅｐ1～ｓｔｅｐ3）、予め設定された閾値と比較する（ｓｔｅｐ4）ことで、オリジナルかコピーかを判定することが可能となる。上記方法は、シンボルパターンをチェックする方法である。

【0109】次に識別情報の位置情報のみを利用してオリジナルかコピーであるかを判定する方法について説明する。

【0110】例えば、図15のように、各行に特定シンボルパターンを挿入しておく。そして、識別情報抽出の際に、何番目のシンボル位置であるかを、各行について検出する。

【0111】そして、それら位置情報をパラメータとして、一方向性関数（図における関数ｇ）に通す。一方向性関数は、異なる入力パラメータに対して、異なる出力をだす。このため、識別情報が挿入された位置情報を複数定めておき、その位置情報から得られる一方向性関数の出力結果ｒと照合することで、オリジナルなもであるかコピーであるかを判定することが可能となる。

【0112】次に、他の識別情報の判定方法について説明する。

【0113】上記判定方法では、メモリや一方向性関数の結果を照合する必要があった。

【0114】そこで、識別情報を予め決めておき、各行に1シンボルだけ挿入する。識別情報抽出の際に、その位置情報をパラメータとして所定の関数g_0に入力する。この関数g_0の出力ｒを一方向関数H_0に入力する。このとき、ｒがある値であれば、すなわち、特定の位置情報をパラメータとした場合は、関数H_0の出力がすべて同じｃになるようにしておく。

【0115】こうすることで、関数H_0の出力がｃであるか否かでオリジナルかコピーであるか判定できる。よって、メモリも必要なくなり、処理時間を短縮することが可能となる。

【0116】＜第5の実施の形態＞これまでの実施形態は、識別情報の位置情報が固定であるか、可変であってもその位置が真に識別情報のシンボル位置であるのか、を確定することが困難で、識別情報の個数などによる統計処理により処理する方法であった。

【0117】そこで、現在新しい著作権保護技術として注目されている電子透かし技術を利用した方法について説明する。

【0118】図17は、本発明の第5の実施の形態に係るコピー防止装置にて使用される情報記録媒体の制作過程を示す図である。

【0119】本実施形態では、識別情報を埋め込むための位置情報をコンテンツに電子透かしとして埋め込むものとする。電子透かしは特徴として、除去しにくく、また取り出しにくいという性質を持つためである。電子透かしについては、「画像深層暗号－手法と応用－」松井著、森北出版株式会社に詳しい。

【0120】さて、アナログ・コンテンツは、A/D 変換回路91にてディジタル情報に変換される。識別情報のための位置情報は電子透かし情報埋め込み回路92にてコンテンツに埋め込まれる。

【0121】図17では、A/D 変換回路91と電子透かし情報埋め込み回路92とが別に示してあるが、多くの透かし埋め込み技術は量子化する際に透かし情報を埋め込むため、A/D 変換回路に透かし情報埋め込み回路を組み込んでおくことが多い。図17では、説明しやすいように別にした。

【0122】識別情報のための位置情報が埋め込まれたコンテンツは、誤り訂正符号化回路93にて誤り訂正符号化される。そして、識別情報が識別情報のための位置情報に従って、識別情報挿入回路94にて一部のコンテンツと入れ替えられる。そして、識別情報が挿入されたコンテンツが情報記録媒体に記録される。

【0123】上記手法を用いれば、識別情報をその都度変化させ、かつ電子透かし技術を用いて位置情報を記録するため、不正に識別情報を埋め込んであるシンボル位置を特定することは困難となる。

【0124】例えば図18のごとく、識別情報を埋め込むための位置情報に従って、識別情報をｉ行目ｕ列のシンボル、ｊ行目ｓ列、ｋ行目ｔ列に埋め込む、ということになる。もちろん場合により、識別情報がデータ部に

のみ埋め込まれる場合や、パリティ部にのみ埋め込まれる場合がある。ただし、識別情報は同じシンボル位置に挿入することがないように気をつける必要がある。

【0125】次に、識別情報の位置を変化させた場合の情報記録媒体の再生について説明する。

【0126】図19は、本発明の第5の実施の形態に係るコピー防止装置を示す図である。なお、図9と同一部分には、同一符号を付し、その説明を省略する。

【0127】DVD ディスク11から、暗号化された鍵情報であるEMki(Dk)とEDk(Dk) が読み出される。そして、これまでと同様に一時鍵生成とデータ暗号鍵の判定が一時鍵＆データ暗号鍵判定部61にて行われ、一時鍵Bkとデータ暗号鍵Dkが得られる。

【0128】復調回路14にて復調処理を受けた暗号化データEDk(Data) は、誤り訂正回路91により誤り訂正処理を受ける。なお、本実施形態では、誤り訂正回路91において内符号、外符号ともに誤り訂正符号化されるものとする。

【0129】暗号化データEDk(Data) の誤り訂正処理中に得られた誤り位置情報と誤りシンボル値とから、誤りパターンが得られる。この誤りパターンを誤りパターン記憶回路92にて記憶する。

【0130】一方、誤り訂正回路91にて誤り訂正が行われた暗号化データEDk(Data) は、バスインターフェースBを通って、復号ユニットC　へ伝送される。伝送された暗号化データEDk(Data) は、一時鍵生成＆データ暗号鍵判定部61にて得られたデータ暗号鍵Dkを用いて復号回路36にて復号される。

【0131】復号回路36において得られたDataには識別情報の埋め込み位置情報が透かし情報として埋め込まれている。復号されたDataは電子透かし情報抽出回路101に入力され、識別情報の位置情報が抽出される。抽出された識別情報の位置情報loc は、一時鍵Bkを復号鍵として復号回路102にて復号され、ディスク・ドライブAへ伝送される。

【0132】ディスク・ドライブAにおける暗号化回路94においては、識別情報の位置情報loc が一時鍵Bkを暗号鍵として暗号回路94にて暗号化され、識別情報の位置情報loc が取り出される。

【0133】そこで、先の誤りパターン記憶回路92に記録された誤りパターンと、識別情報の位置情報loc とから、識別情報抽出回路93にて識別情報DIが抽出される。この識別情報DIから識別情報判定回路95にてディスクがオリジナルかコピーかが判定され、判定結果を示す制御信号CS2 が出力される。

【0134】出力された制御信号CS2 は、暗号回路96にて一時鍵Bkを暗号鍵として暗号化され、復号ユニットCへ伝送される。復号ユニットCでは、復号回路103　にて一時鍵Bkを復号鍵として復号し、制御信号CS2 を得る。

【0135】例えば、D/A 変換回路の手前で、タッピングなどの技術を用いてデータを取り、記録したディスクであるならば、誤り訂正回路91を通っているので、識別情報は存在しない。

【0136】すなわち、識別情報は、識別情報と入れ替える前のシンボルに変わっているはずである。従って、識別情報は特定位置にはなく、コピーされたディスクであることが判定できる。

【0137】このように、識別情報判定回路95は、コピーされたか、オリジナルであるかを判定し、コピー可能か不可能かを示す制御信号CS2 を出力する。コピー防止回路40は、制御信号CS2 を利用して、オリジナル・ディスクとコピー管理信号とから、コピー可能か否かを判定し、コピー不可能であればコピーできないようにする。

【0138】復号回路36にて復号された暗号化データDataは、伸長回路37にて圧縮されたデータが伸長され、さらにD/A 変換回路38にてアナログデータに変換されて、ディスプレイやスピーカ（図示せず）を通して再生される。

【0139】この様に透かし情報を利用することにより、識別情報の位置情報を可変にし、かつ秘密裏に積符号内に識別情報を埋め込むことが可能となる。

【0140】＜制御信号を安全に伝送する方法＞次に、制御信号CS2 を安全に伝送する方法について述べる。

【0141】制御信号CS2 はオリジナルかコピーかを示す信号であり、少なくとも1ビットあれば済む。例えば、"0" であればコピー、"1" であればオリジナル、という設定が考えられる。これは逆でも構わない。

【0142】このように少ないビットを暗号化した場合、元のデータ（暗号学上では平文）を長い鍵で暗号化しても、解読されやすい、という性質がある。

【0143】従って、バス上を一時鍵で暗号化したとしても、解読されてしまう恐れがある。ここで、制御信号CS2 を安全に伝送する方法について、図20を用いて説明する。

【0144】図20において、Aはディスク・ドライブ、Bはバスインターフェース、Cは復号ユニットである。なお、図20では、必要な部分のみを図示している。

【0145】これまで示してきた実施形態において、識別情報DIが取り出されたものとする。この識別情報DIは、識別情報判定回路111にて判定され、判定結果を示す制御信号CS2 が出力される。

【0146】一方、乱数生成回路112にて乱数R が生成され制御信号CS2 との排他論理和演算が行われる。また、乱数R は暗号回路115にて一時鍵Bkにて暗号化され、暗号化された乱数EBK(R)が復号ユニットCにおける復号回路122に伝送される。

【0147】また乱数R と制御信号CS2 との排他論理和

R'も同様に暗号回路１１４にて一時鍵Bkで暗号化され、暗号化された排他的論理和R'が復号ユニットＣの復号回路１２１に伝送される。

【０１４８】復号ユニットＣでは、伝送された暗号化された乱数EBK(R)を復号回路１２２において一時鍵Bkで復号し、復号回路１２１において暗号化された排他論理和の結果であるEBK(R') を一時鍵Bkで復号する。

【０１４９】そして、乱数R と排他論理和の結果であるR'を得て、この２つの排他論理和演算を行うことで、制御信号CS2 を取り出すことができる。この乱数のビット長は、暗号化を行うときの入力ビット長と同じにしておけば良い。

【０１５０】ここで、図２０における乱数生成回路を使用せず、一時鍵生成で使用される乱数を使用しても良い。この一時鍵の生成で使用される乱数は、ディスク・ドライブ、復号ユニットの両方で共有される乱数であるので、図２０のような乱数を暗号化して送る手順を省くことができる。

【０１５１】また、乱数生成回路により生成される乱数が暗号などで使用される条件、任意の長さでの全系列の等頻度性、無相関性、長周期性、非線型性、予測不可能性、といった諸条件を満足するものであるならば、暗号回路１１４、復号回路１２１を省略することもでき、処理手順や回路を簡単にすることができる。

【０１５２】＜識別情報の特定＞次に、識別情報を特定するための方法について説明する。

【０１５３】ここで述べる識別情報を特定するための方法は、DVD におけるCSS(Content Scramble System)というシステムを利用した方法である。CSS については、前述した「DVD 、パソコン載る」日経エレクトロニクス、1997.8.18(no.696) , p.110-120 に説明されている。

【０１５４】文献に依れば、DVD ディスクのリードイン領域という特殊な領域（論理ファイル・システムからはアクセスできない領域）があり、そこに暗号化された鍵情報を格納する領域がある。

【０１５５】そこで、この暗号化された鍵情報EMki(Dk),EDk(Dk)を利用して識別情報の位置情報を特定する方法を図２１に示す。なお、図２１では、ディスク・ドライブの必要な部分のみを図示している。

【０１５６】さて、DVD ディスク１３１から暗号化された鍵情報EMki(Dk), EDk(Dk) が読み出され、ハッシュ関数（データを圧縮する関数）１３５を用いて圧縮される。この圧縮された鍵情報EMki(Dk), EDk(Dk) が識別情報の位置情報loc となる。

【０１５７】従って、この方法を使用した場合には、ディスク内の全ての積符号ブロックにおいて、識別情報の挿入位置が固定となる。ただし、ディスクが異なれば識別情報の挿入位置を異なる位置にすることも可能である。

【０１５８】従って、識別情報を挿入する位置は、コンテンツ・データを誤り訂正符号化して、識別情報を挿入する前に、この記録するディスクの鍵情報EMki(Dk), EDk(Dk) とハッシュ関数とを用いて予め計算しておき挿入する必要がある。このときハッシュ関数は、鍵情報EMki(Dk), EDk(Dk) を入力したときに、必ず積符号ブロックの誤り訂正符号長さ以下となる必要がある。

【０１５９】ハッシュ関数１３５により変換された暗号化された鍵情報EMki(Dk), EDk(Dk)は、識別情報の位置情報loc となる。一方、読み出された暗号化データEDk(Data) は、復調回路１３２にて復調処理を受け、誤り訂正回路１３３により誤り訂正処理を受ける。なお、誤り訂正回路１３３において内符号、外符号ともに誤り訂正されるものとする。

【０１６０】暗号化されたデータEDk(Data) の誤り訂正処理中に得られた誤り位置情報と誤りシンボル値とから、誤りパターンが得られる。この誤りパターンは、誤りパターン記憶回路１３４にて記憶される。

【０１６１】そして、識別情報の位置情報loc と、誤りパターン記憶回路１３４に記憶された誤りパターンとから、識別情報DIが抽出される。

【０１６２】＜識別情報の訂正＞次に、識別情報そのものが誤り訂正符号である場合について説明する。

【０１６３】すなわち、上述の実施の形態において、識別情報が誤り訂正符号である場合である。

【０１６４】図２２は、識別情報に誤り訂正符号を使用した場合の識別情報の判定処理を説明するためのフローチャートである。

【０１６５】同図に示すように、識別情報が検出される（step１１）と、この検出された識別情報に対して、その誤り訂正能力を使用して誤り訂正が行われる（ｓｔｅｐ１２）。

【０１６６】そして、次に、この誤り訂正が施された識別情報に対して、識別情報の決定が行われる（ｓｔｅｐ１３）。従って、識別情報に誤り訂正符号を使用した場合には、復調された識別情報自体に誤りが存在していても、その誤り訂正能力を使用して識別情報を訂正するので、より正確に識別情報が存在するか否かを決定することができる。

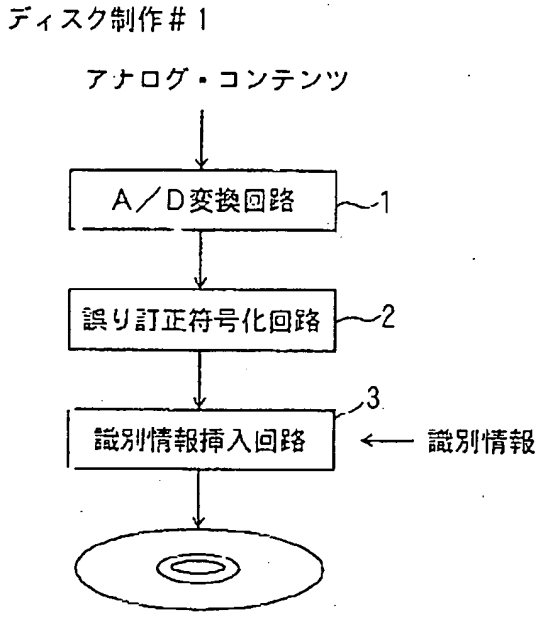
【０１６７】

【発明の効果】以上詳記したように、本発明によれば、誤り訂正符号にオリジナルの記録媒体であるのかを示す識別信号を、誤りとして挿入することにより、誤り訂正処理前にその識別情報を抽出することで、オリジナルな記録媒体であるかを判定することが可能となる。

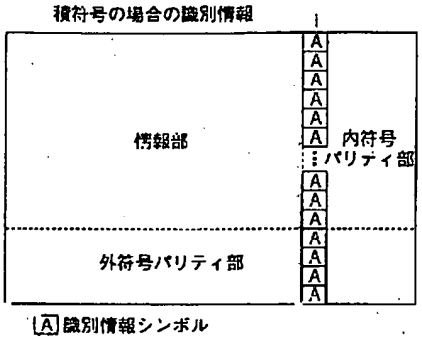
【０１６８】また、誤り訂正処理を終えれば、識別情報は誤りとして処理されるため、元の正しいシンボルに訂正される。このため、再生処理途中でデータをコピーしたとしても、オリジナルであるための識別情報が失われるため、不正なコピーをした情報記録媒体を役に立たせなくすることが可能となる。

【図面の簡単な説明】
【図１】本発明の第１の実施形態におけるコピー防止装置において使用されるディスクの制作の過程を説明するための図。
【図２】識別情報の挿入方法について説明するための図。
【図３】本発明の第１の実施の形態に係るコピー防止装置を示す図。
【図４】一般的な積符号の符号化および復号化の流れを示す図。
【図５】積符号を使用した場合の情報記録媒体の製造手順を示す図。
【図６】本発明の第２の実施の形態に係るコピー防止装置を示す図。
【図７】本発明の第３の実施の形態に係るコピー防止装置において使用される情報記録媒体の製造方法を示す図。
【図８】本発明の第３の実施の形態に係るコピー防止装置を示す図。
【図９】本発明の第４の実施の形態に係るコピー防止装置を示す図。
【図１０】識別情報の挿入方法を説明するための図。
【図１１】識別情報の挿入方法を説明するための図。
【図１２】識別情報の挿入方法を説明するための図。
【図１３】識別情報の挿入方法を説明するための図。
【図１４】識別情報の判定方法を説明するためのフローチャート。
【図１５】識別情報の挿入方法を説明するための図。
【図１６】識別情報の挿入方法を説明するための図。
【図１７】本発明の第５の実施の形態に係るコピー防止装置にて使用される情報記録媒体の制作過程を示す図。
【図１８】識別情報の挿入方法を説明するための図。
【図１９】本発明の第５の実施の形態に係るコピー防止装置を示す図。
【図２０】制御信号を安全に伝送する方法を説明するための図。
【図２１】鍵情報を利用して識別情報の位置を特定するための方法を説明するための図。
【図２２】識別情報に誤り訂正符号を使用した場合の識別情報の判定処理を説明するためのフローチャート。
【符号の説明】
１…A/D 変換回路、
２…誤り訂正符号化回路、
３…識別情報挿入回路、
１１…DVD ディスク、
１２…復調／誤り訂正回路、
１３…暗号化回路、
１４…復調回路、
１５…誤り訂正回路、
１６…誤りパターン記憶回路、
１７…識別情報判定回路、
１８…暗号回路、
３１…鍵メモリ、
３２…復号回路、
３３…復号回路、
３４…復号回路、
３５…判定回路、
３６…復号回路、
３７…伸長回路、
３８…Ｄ／Ａ変換回路、
３９…復号回路、
４０…コピー防止回路、
５１…A/D 変換回路、
５２…内符号符号化回路、
５３…識別情報挿入回路、
５４…外符号符号化回路、
５５…変調回路、
６１…一時鍵＆データ暗号鍵判定部、
６２…外符号誤り訂正回路、
６３…識別情報メモリ、
６４…識別情報検出回路、
６５…識別情報判定回路、
６６…内符号誤り訂正回路、
７１…外符号誤り訂正回路、
７２…内符号誤り訂正回路、
７３…誤りパターン記憶回路、
７４…識別情報メモリ、
７５…識別情報検出回路、
７６…識別情報判定回路、
８１…識別情報メモリ、
８２…識別情報検出回路、
８３…暗号回路、
８４…外符号誤り訂正回路、
８５…内符号誤り訂正回路、
８６…復号回路、
８７…識別情報判定回路、
９３…識別情報抽出回路、
９５…識別情報判定回路、
１０１…電子すかし情報抽出回路、
１１１…識別情報判定回路、
１１２…乱数生成回路。

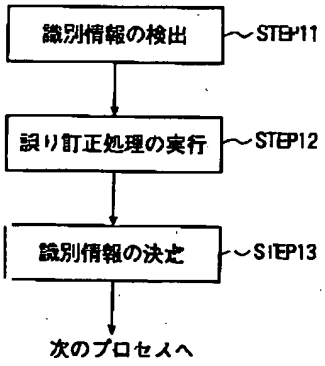
【図1】



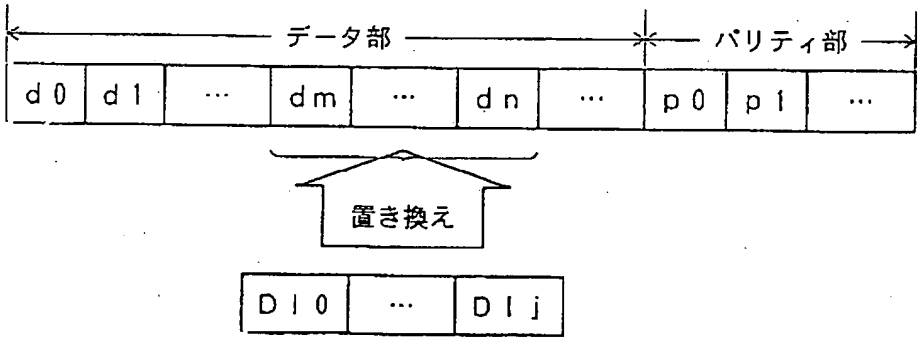
【図10】



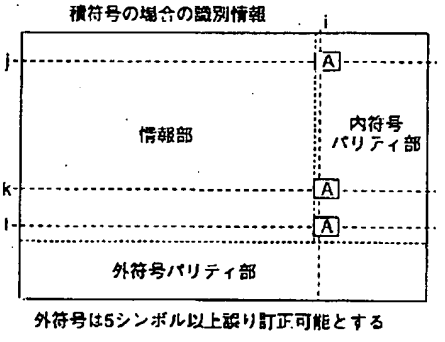
【図22】



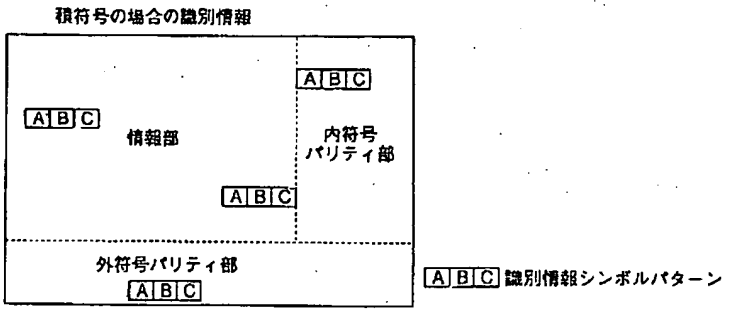
【図2】



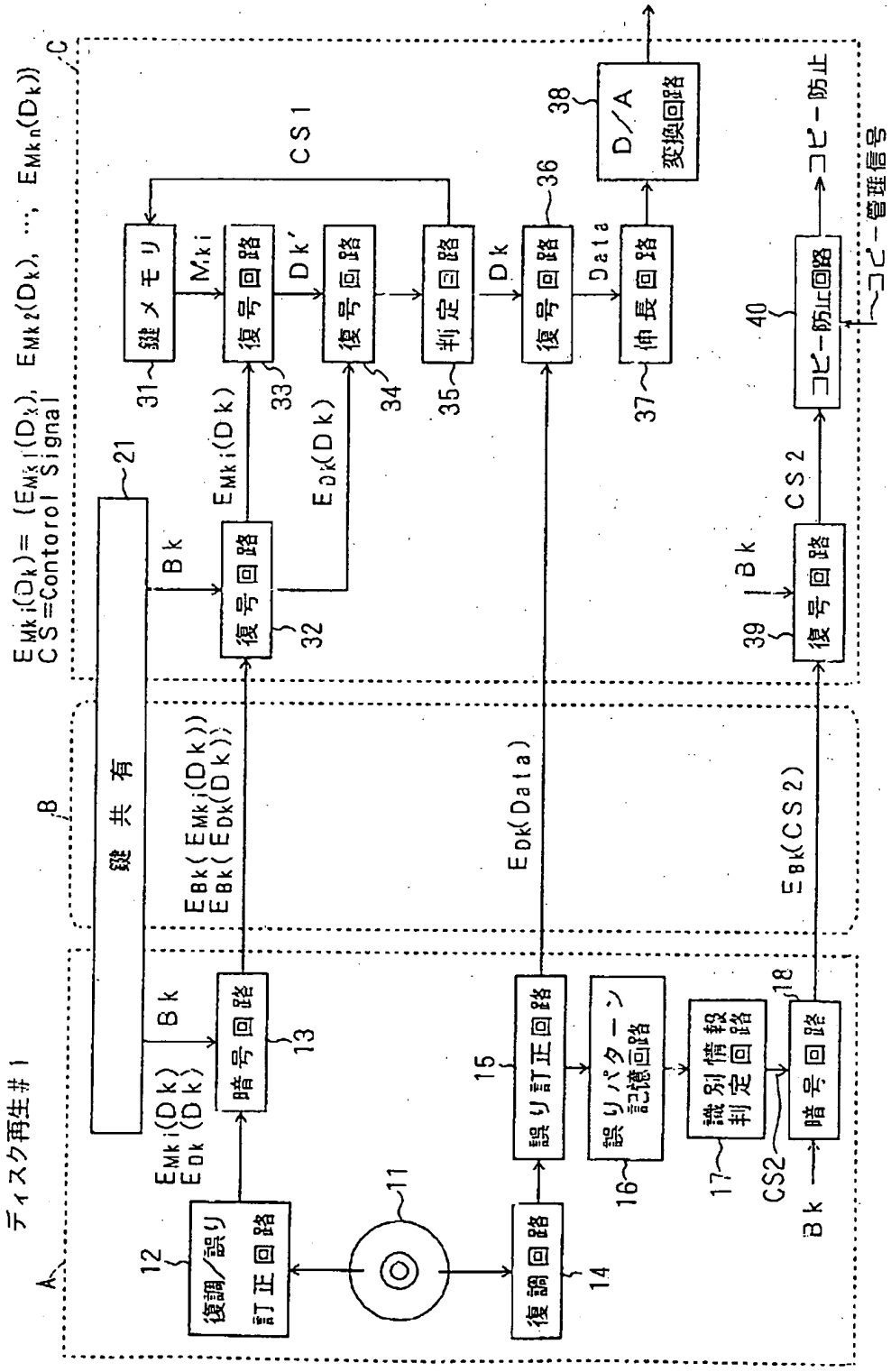
【図11】



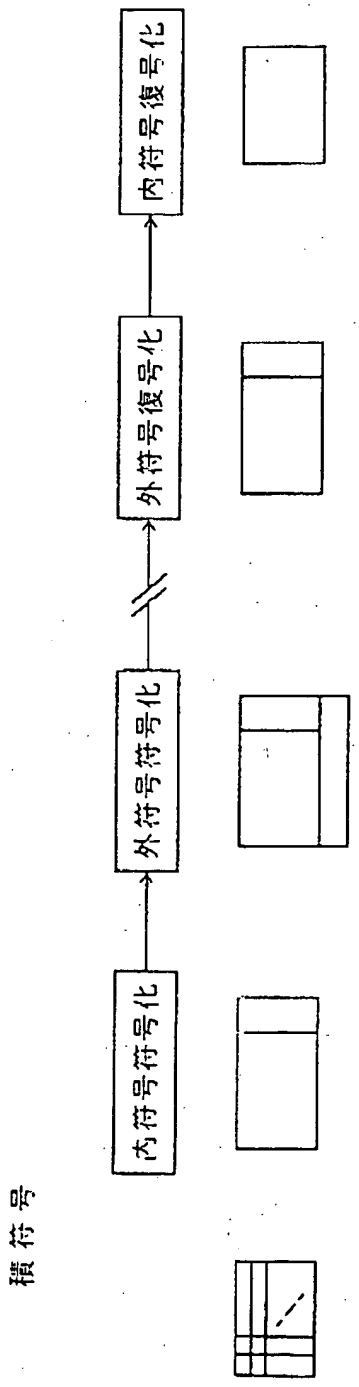
【図12】



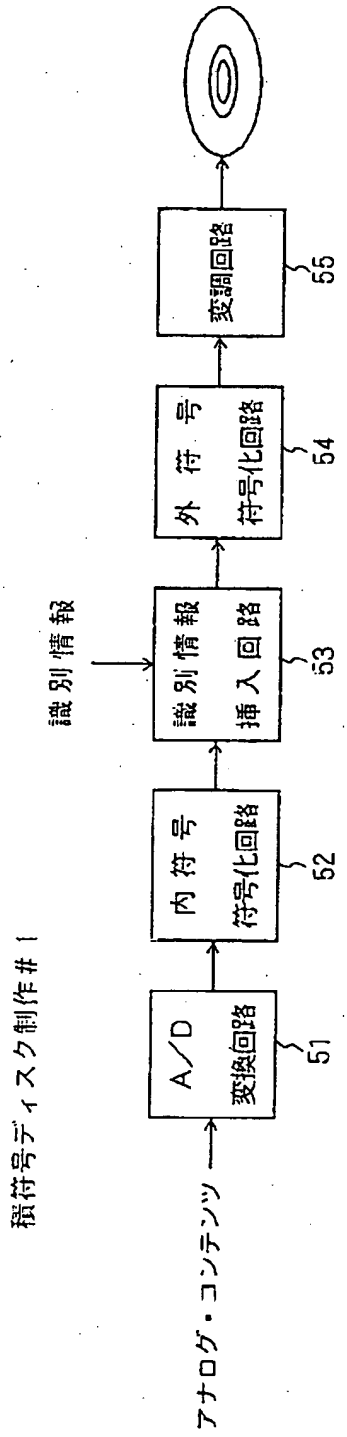
【図3】


ディスク再生#1
A
B
C
鍵共有
$E_{Mki}(D_k)=(E_{Mk1}(D_k), E_{Mk2}(D_k), \cdots, E_{Mkn}(D_k))$
CS=Contorol Signal
$E_{Mki}(D_k)$
$E_{Dk}(D_k)$
Bk
12 復調/誤り訂正回路
11
13 暗号回路
14 復調回路
15 誤り訂正回路
16 誤りパターン記憶回路
17 識別情報判定回路
18 暗号回路
CS2
Bk
21
$E_{Bk}(E_{Mki}(D_k))$
$E_{Bk}(E_{Dk}(D_k))$
$E_{Dk}(Data)$
$E_{Bk}(CS2)$
31 鍵メモリ
Mki
32 復号回路
33 復号回路
Dk'
34 復号回路
35 判定回路
Dk
36 復号回路
Data
37 伸長回路
38 D/A変換回路
CS1
39 復号回路
Bk
CS2
40 コピー防止回路
コピー防止
コピー管理信号

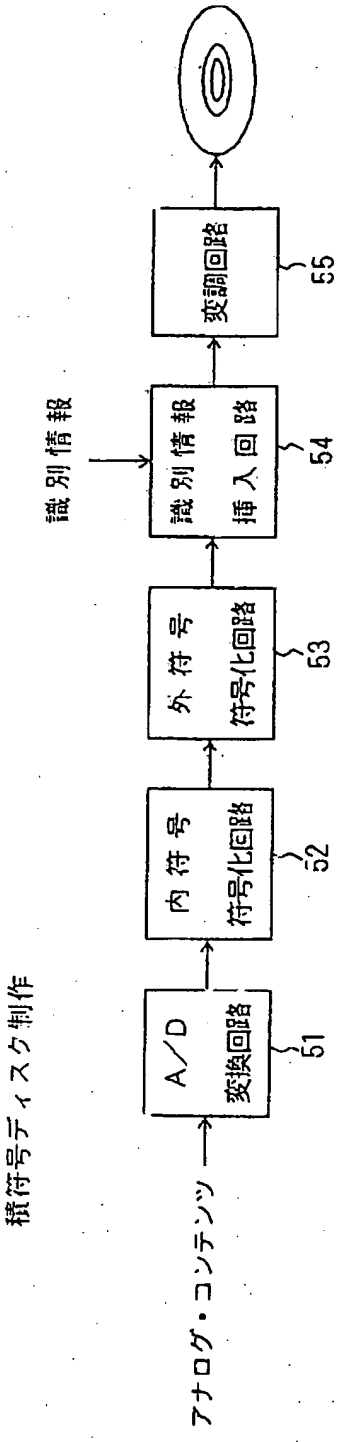
【図4】


積符号
内符号符号化
外符号符号化
外符号復号化
内符号復号化

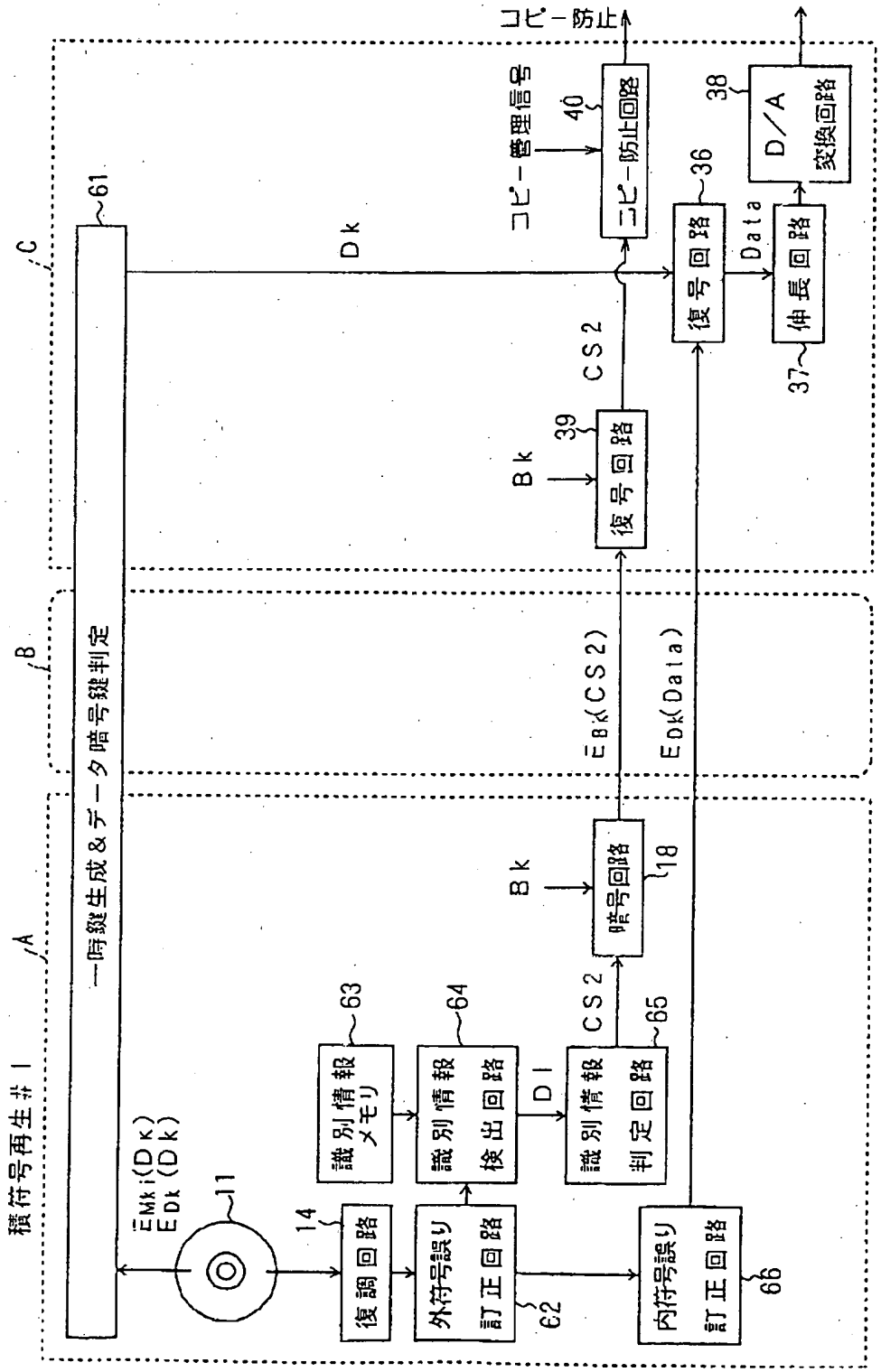
【図5】


積符号ディスク制作#1
アナログ・コンテンツ
A／D 変換回路 51
内符号 符号化回路 52
識別情報
識別情報 挿入回路 53
外符号 符号化回路 54
変調回路 55

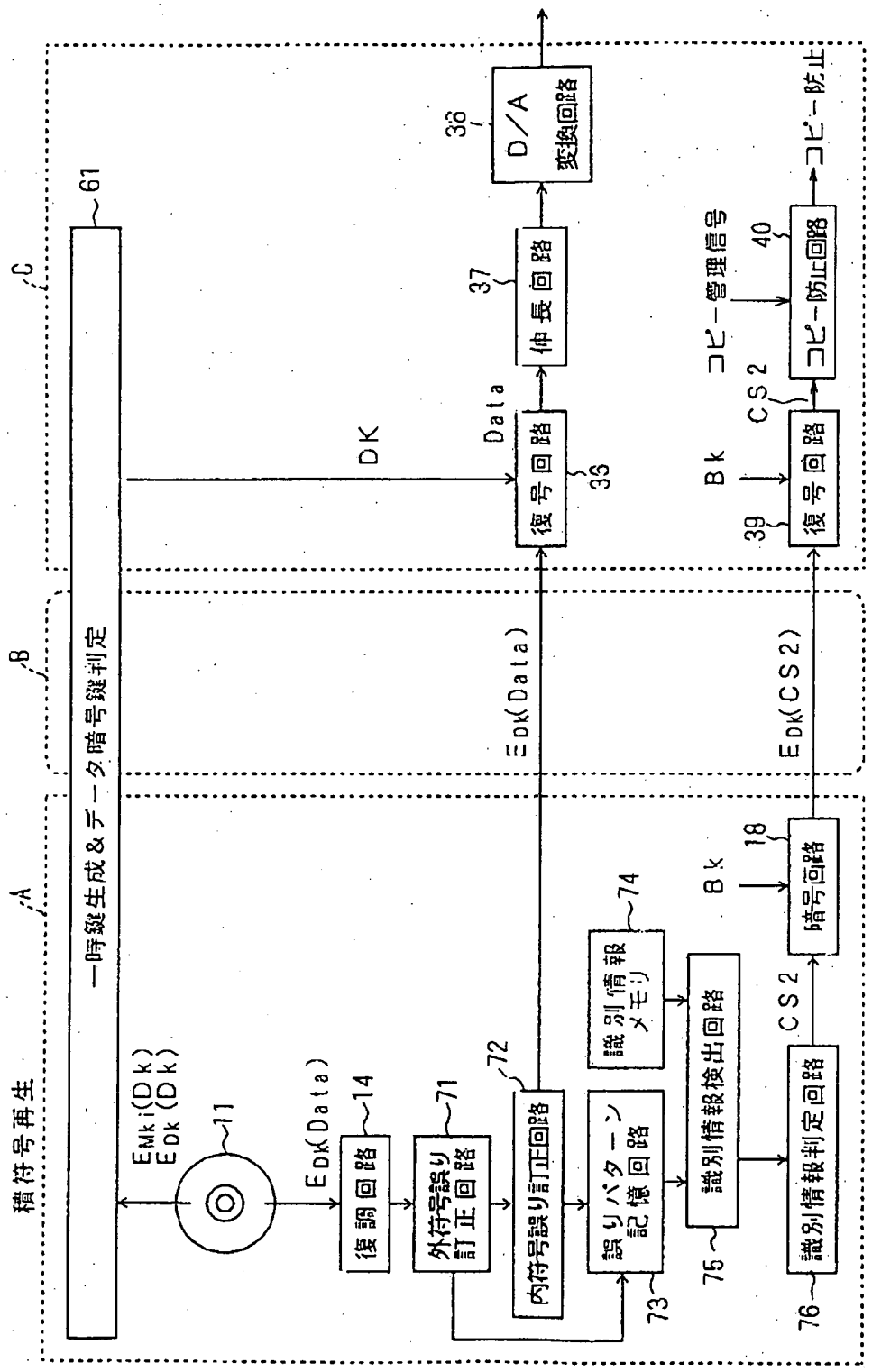
【図7】


積符号ディスク制作
アナログ・コンテンツ
A／D 変換回路 51
内符号 符号化回路 52
外符号 符号化回路 53
識別情報
識別情報 挿入回路 54
変調回路 55

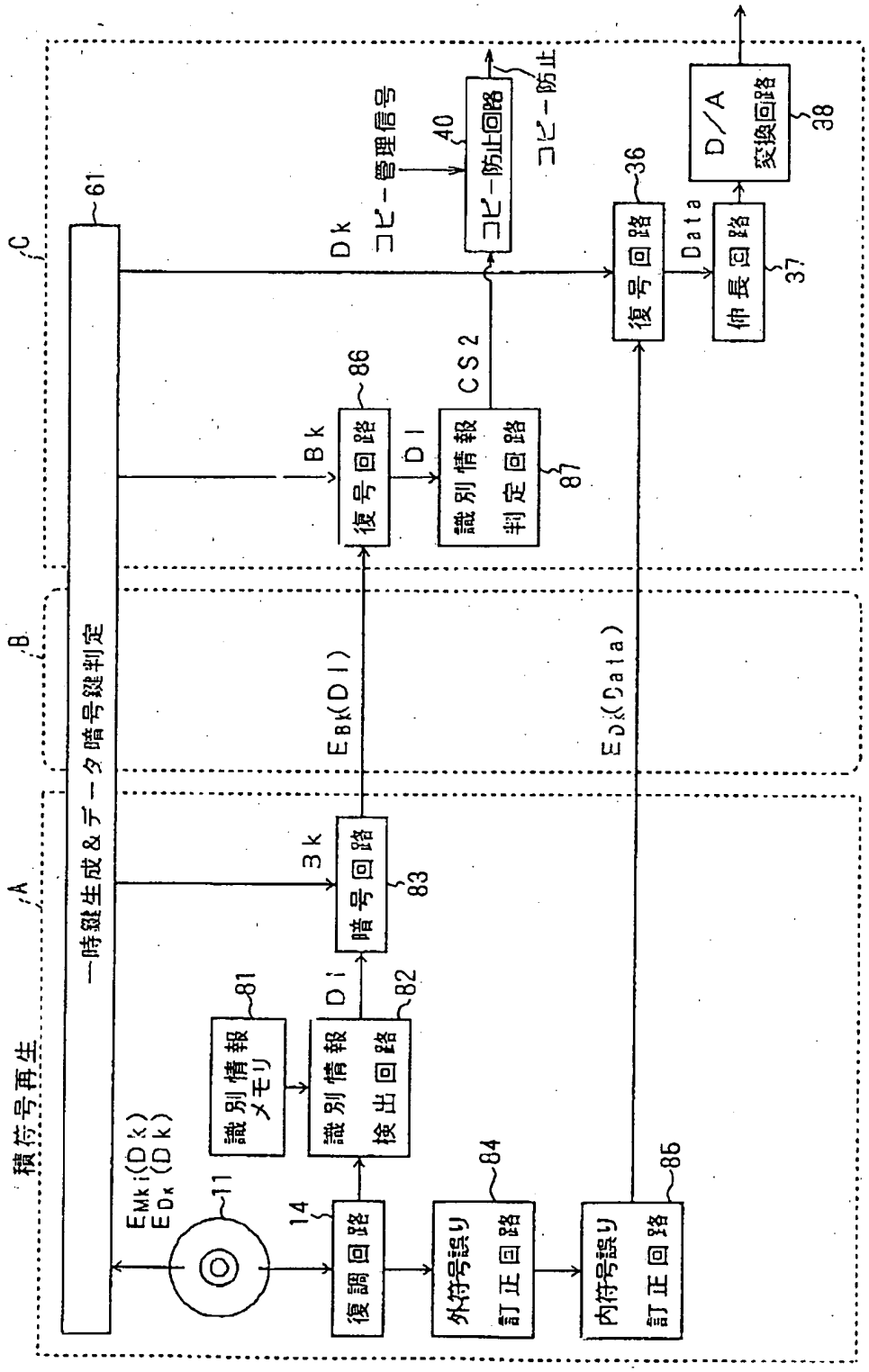
【図6】


積符号再生ボ1
A
B
C
一時鍵生成＆データ暗号鍵判定
EMki(Dk)
EDk(Dk)
11
14
復調回路
識別情報メモリ
63
識別情報検出回路
64
外符号誤り訂正回路
62
DI
CS2
識別情報判定回路
65
内符号誤り訂正回路
66
Bk
暗号回路
18
EBk(CS2)
EDk(Data)
Bk
39
復号回路
CS2
Dk
61
コピー管理信号
40
コピー防止回路
コピー防止
復号回路
36
Data
伸長回路
37
D/A
変換回路
38

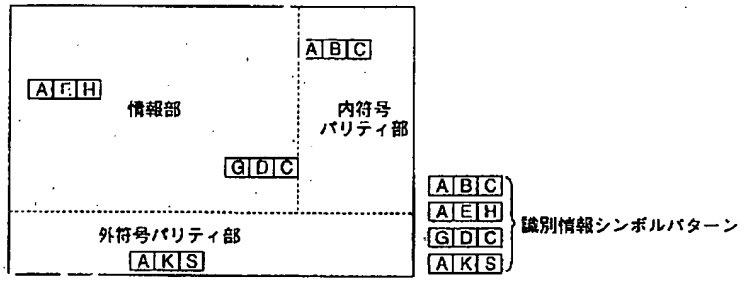
【図8】


積符号再生
A
B
C
一時鍵生成＆データ暗号鍵判定
61
11
EMki(Dk)
EDk(Dk)
EDk(Data)
復調回路
14
外符号誤り訂正回路
71
内符号誤り訂正回路
72
誤りパターン記憶回路
73
識別情報メモリ
74
識別情報検出回路
75
識別情報判定回路
76
CS2
暗号回路
18
Bk
EDk(Data)
EDk(CS2)
DK
Data
復号回路
33
伸長回路
37
D/A変換回路
38
Bk
CS2
復号回路
39
コピー管理信号
コピー防止回路
40
コピー防止

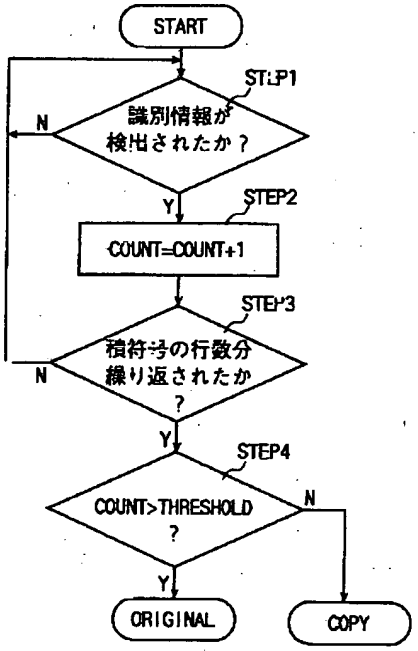
【図9】


積符号再生
A
B
C
一時鍵生成＆データ暗号鍵判定
61
11
14
復調回路
外符号誤り訂正回路
84
内符号誤り訂正回路
86
識別情報メモリ
81
識別情報検出回路
82
暗号回路
83
復号回路
86
識別情報判定回路
87
コピー防止回路
40
コピー防止
復号回路
36
伸長回路
37
D／A変換回路
38
Dk
コピー管理信号
CS2
Bk
DI
Di
3k
Data
EMki(Dk)
EDk(Dk)
EBk(DI)
EDk(Data)

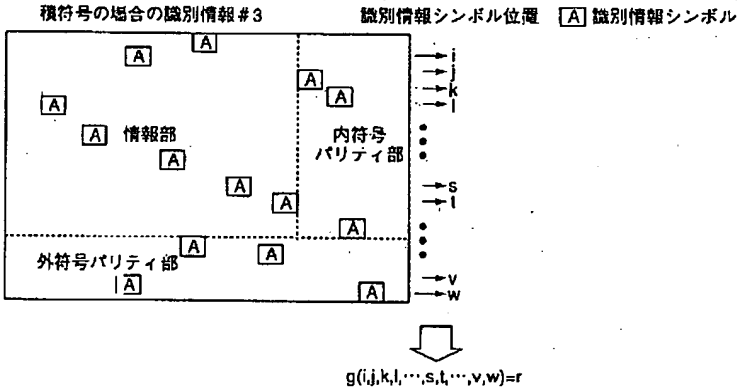
【図13】



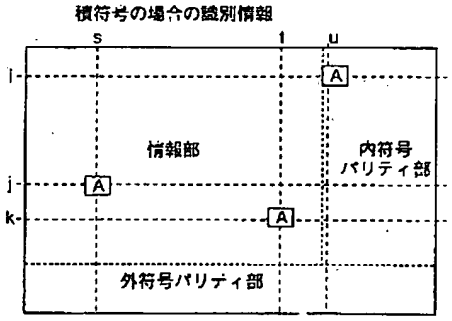
【図14】



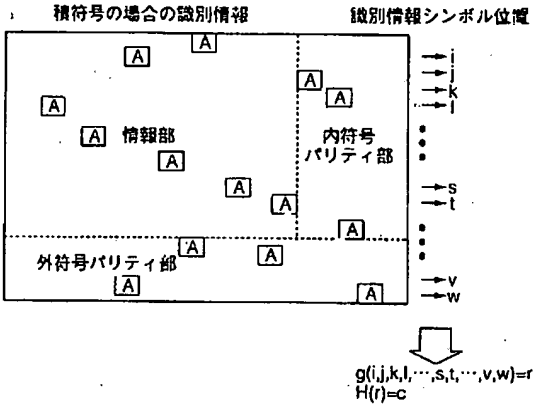
【図15】



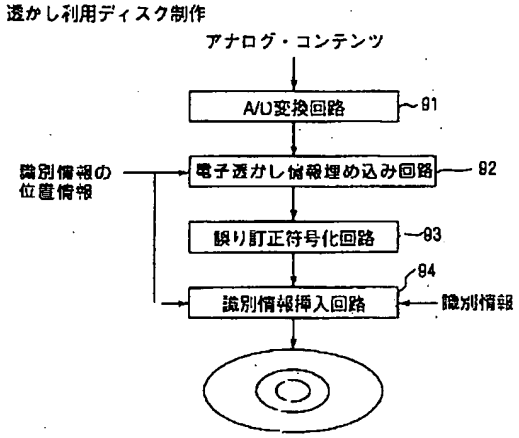
【図18】



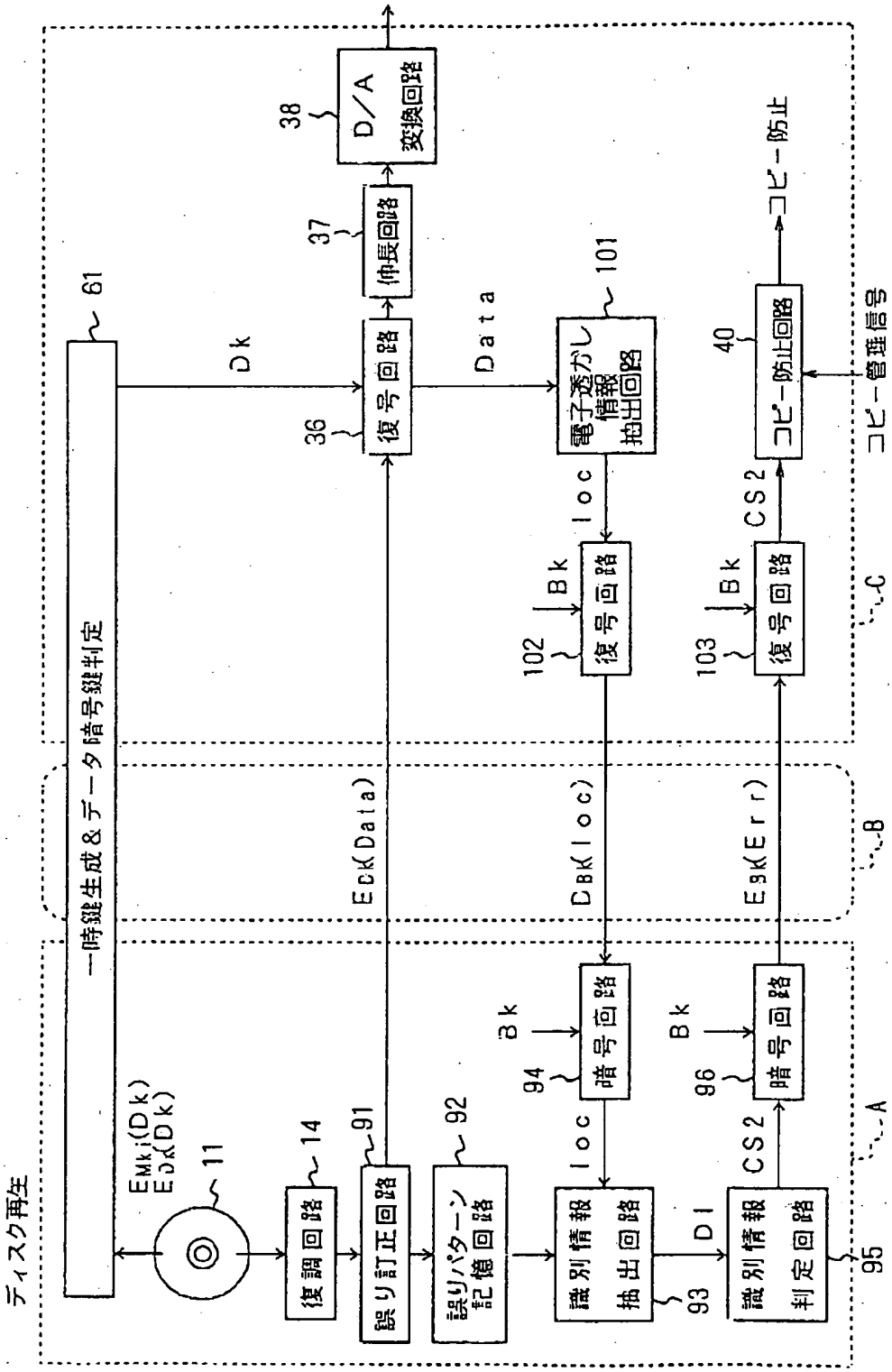
【図16】



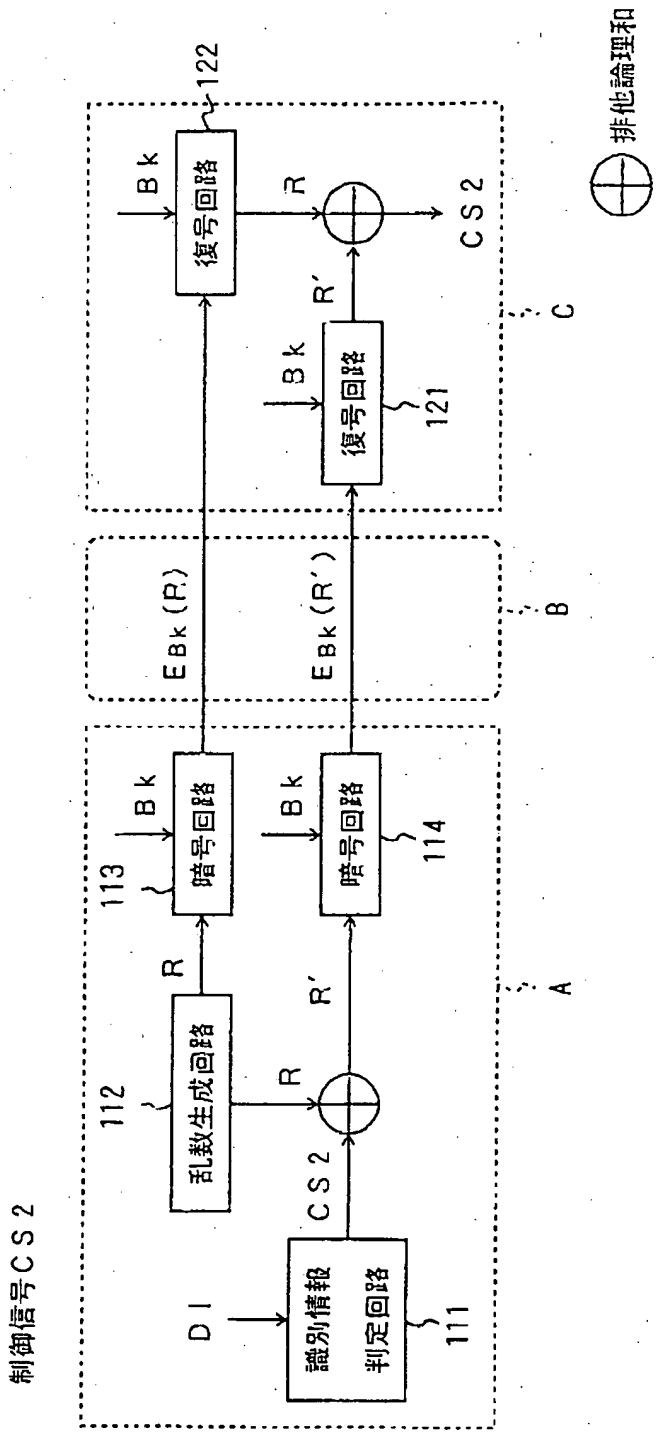
【図17】



【図19】

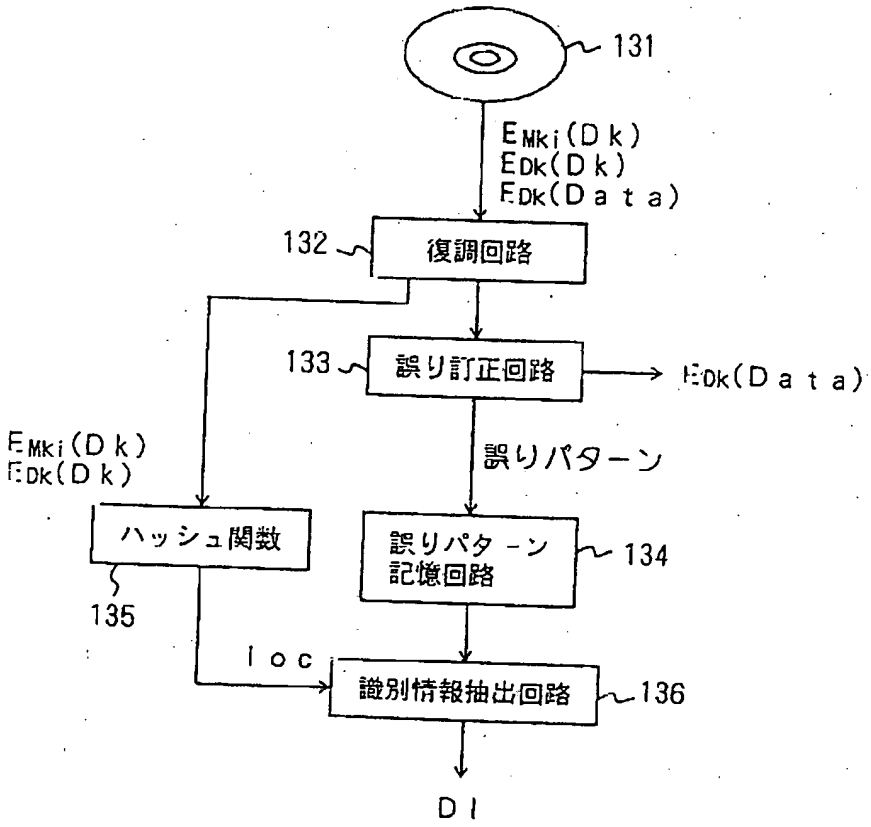

ディスク再生
一時鍵生成＆データ暗号鍵判定
61
$E_{Mkj}(Dk)$
$E_{DK}(Dk)$
11
復調回路
14
誤り訂正回路
91
誤りパターン記憶回路
92
識別情報抽出回路
93
識別情報判定回路
95
暗号回路
94
暗号回路
96
Dk
Bk
Ioc
DI
CS2
復号回路
36
伸長回路
37
D／A変換回路
38
Data
電子透かし情報抽出回路
101
復号回路
102
復号回路
103
コピー防止回路
40
コピー管理信号
$E_{DK}(Data)$
$D_{BK}(Ioc)$
$E_{BK}(Err)$
A
B
C

【図20】


制御信号CS2
DI
識別情報判定回路
111
CS2
乱数生成回路
112
R
R'
暗号回路
113
暗号回路
114
Bk
Bk
EBk(R)
EBk(R')
A
B
C
復号回路
121
復号回路
122
Bk
Bk
R'
R
CS2
排他論理和

【図21】

識別情報の位置情報の特定



フロントページの続き

(72)発明者　山田　尚志
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(72)発明者　遠藤　謙二郎
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内